ОБЩИНА ДОСПАТ

4831, гр. Доспат, обл. Смолян
ул. „Кап. Петко Войвода" № 3
Тел.: 03045/23 10, факс: 03045/ 23 12

MUNICIPALITY OF DOSPAT

4831, Dospat, Smolian Region
3 „Kap. Petko Voivoda" Str.
Phone: 03045/23 10, Fax: 03045/ 23 12

Web: www.dospat.bg, e-mail: obshtina.dospat@dospat.egov.bg

УТВЪРДИЛ: .....

ИНЖ. ЕЛИН РАДЕВ

КМЕТ НА ОБЩИНА ДОСПАТ

ОБЩИНА ДОСПАТ

Вътрешни правила за класификация на информацията

ГЛАВА ПЪРВА

Раздел I

ОБЩИ ПОЛОЖЕНИЯ

Чл.1. Тези правила имат за цел да укажат как се маркира, използва, обработва, обменя, съхранява и унищожава информацията, с която разполага Община Доспат.

Чл.2. Приети са въз основа на чл. 5, ал. 1, т. 6 и 7 от Наредбата за минимални изисквания за мрежова и информационна сигурност (Наредбата).

Чл.3. Правилата целят гарантирането на достатъчна, адекватна и пропорционална на заплахите защита на информацията с оглед на нейната важност, чувствителност и на нормативните изисквания към нея.

Чл.4. Класификацията се прилага и върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето и унищожаването на информацията, като към тях трябва да се прилагат подходящи механизми за защита, съответстващи на идентифицираните заплахи.

Чл.5. (1) Община Доспат нанася нивото на класификацията по подходящ начин върху документираната информация.

(2) За класификацията не се използват нивата на класификация за сигурност на информацията от обхвата на Закона за защита на класифицираната информация, както и техният гриф.

(3) Информацията без класификация е достъпна за общо ползване при спазване на стандартните правила за авторски права и към нея не се прилагат механизми за защита.

(4) При обмен на информация се използва класификация TLP (traffic light protocol) съгласно приложение № 2 от Наредбата.

Раздел II

КЛАСИФИКАЦИИ НА ИНФОРМАЦИЯТА

Чл.6. (1) С цел да се гарантира достатъчна, адекватна и пропорционална на заплахите защита на информацията, се прави преценка на важността и чувствителността ѝ, както и на нормативните изисквания към нея.

(2) Въз основа на тази преценка информацията се разделя в няколко категории. Когато е приложимо, тази класификация се пренася и върху всички ресурси, които участват в създаването, обработването, съхраняването, пренасянето, разпространението и унищожаването на информацията, и към тях се прилагат подходящи мерки за защита, съответстващи на заплахите.

Чл.7. При обмен на информация се използва TLP (traffic light protocol):

1. [TLP-RED] – Само за определени получатели: в контекста на една среща например информацията се ограничава до присъстващите на срещата. В повечето случаи тази информация се предава устно или лично.
2. [TLP-AMBER] – Ограничено разпространение: получателят може да споделя тази информация с други хора от организацията, но само ако е спазен принципът "необходимост да се знае". Честа практика е източникът на информацията да уточни веднага след маркировката на кого може да се споделя информацията или да предвиди ограничения на това споделяне. Ако получателят на информацията иска да я разпространява, задължително трябва да се консултира с източника.
3. [TLP-GREEN] – Широка общност: информацията в тази категория може да бъде разпространявана широко в рамките на дадена общност. Въпреки това информацията не може да бъде публикувана или поствана в интернет, както и изнасяна извън общността.
4. [TLP-WHITE] – Неограничено: предмет на стандартните правила за авторско право; тази информация може да се разпространява свободно, без ограничения.

Чл.8. В Общината се спазва препоръчителната класификация на информацията и изисквания към информационните и комуникационните системи за осигуряване на достъп до информацията от Наредбата:

1. "Ниво 0" обхваща открита и общодостъпна информация (например публикувана на интернет страниците); предполага анонимно ползване на информацията и липса на средства за защита на конфиденциалността ѝ; отговаря на TLP-WHITE;
   a) оповестяването на информация с класификация "Ниво 0" не е ограничено;
   b) източниците могат да използват класификация "Ниво 0", когато информацията носи минимален или никакъв предвидим риск от злоупотреба, в съответствие с приложимите правила и процедури за публично оповестяване;
   c) при спазване на стандартните правила за авторски права информация с класификация "Ниво 0" може да се разпространява без ограничения.
2. "Ниво 1"обхваща:
   a) споделянето на информация с класификация "Ниво 1" е ограничено само до дадена общност; отговаря на TLP-GREEN;
   b) източниците могат да използват класификация "Ниво 1", когато информацията е полезна за информираността на всички участващи организации, както и за партньори от широката общност или сектор;
   c) получателите могат да споделят информация с класификация "Ниво 1" с партньорски организации в рамките на своя сектор или общност, но не и чрез обществено достъпни канали; информацията в тази категория може да се разпространява широко в дадена общност, но не и извън нея;
   d) изисквания към информационните и комуникационните системи:
   e) достъпът до точно определени обекти да бъде разрешаван на точно определени ползватели;
   f) ползвателите да се идентифицират, преди да изпълняват каквито и да са действия, контролирани от системата за достъп; за установяване на идентичността трябва да се използва защитен механизъм от типа

b) източниците могат да използват класификация "Ниво 3", когато информацията не може да бъде ефективно обменяна с други страни и би могла да доведе до въздействия върху неприкосновеността на личния живот, репутацията или операциите на дадена страна, ако с нея бъде злоупотребено;
c) получателите не могат да споделят информация, маркирана с "Ниво 3", с която и да е страна извън конкретния обмен, обработка или съхранение; достъпът до информацията с класификация "Ниво 3" е ограничен само до лицата, участващи в обработката ѝ; в повечето случаи информация с класификация "Ниво 3" трябва да се предава лично;
d) изисквания към ИКТ системите – в допълнение към изискванията към предишното ниво:
e) като механизъм за идентификация да се използва единствено удостоверение за универсален електронен подпис;
f) при издаване на удостоверението да е гарантирана физическата идентичност на лицето;
g) доверителната изчислителна система трябва да бъде с проверена устойчивост към опити за проникване;
h) комуникацията между потребителя и системата да се осъществява по криптирани канали, използващи протокол Transport Layer Security (TLS) поне 1.2, като минималната дължина на криптиращия ключ трябва да е поне 256 бита;
i) доверителната изчислителна система да има механизъм за регистрация на опити за нарушаване политиката за сигурност.

Раздел III

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Ръководителите и служителите в Община Доспат са длъжни да познават и спазват разпоредбите на тези правила.

§ 2. Контролът по спазване на правилата се осъществява от Секретаря на Общината. Допустими са допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защита на информацията.

§ 3. Настоящите вътрешни правила се разглеждат и оценяват периодично с оглед ефективността им, като Община Доспат може да приема и прилага допълнителни мерки и процедури, които са целесъобразни и необходими с оглед защитата на информацията.

§ 4. Тези правила са разработени съгласно Наредба за минималните изисквания за мрежова и информационна сигурност и са утвърдени със заповед на кмета на общината № ..А-613...../..22.10.....2020 г.

Изготвил:

Инж. Веселин Калфов

Секретар на Община Доспат и ССИ